

REMARKS

This Response is submitted in answer to the Office Action dated November 16, 2005, having a shortened statutory period set to expire February 16, 2005.

In the present Office Action, Claims 1-16 are rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the enablement requirement. Specifically, Examiner believes that the feature of "interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device" as previously recited in Claims 4, 9, and 14 is not described in the specification.

In response, Applicants have amended Claims 1-16 to clarify the difference between a "configuration password" (Specification, page 7, lines 24-25) and a "device password" (Specification, page 10, lines 3-18). Specifically, Applicants have changed "password information" to "device password" in Claims 1-16. Therefore, Examiner's rejection of Claims 1-16 under § 112, first paragraph has now been rendered moot, and Applicants respectfully request that the rejection be withdrawn in light of the amendments to Claims 1-16. Applicants also believe that the abovementioned arguments render Examiner's rejection of Claims 1-16 under § 112, second paragraph, moot and respectfully request that rejection be also withdrawn in light of the amendments to Claims 1-16.

In paragraph 5 of the present Office Action, Claims 1-3, 7-8, and 12-13 are rejected under 35 U.S.C. § 102(b) as unpatentable over U.S. Patent No. 6,484,308 B1 to *Pearce et al. (Pearce)*. After careful consideration of Examiner's remarks, Applicants respectfully submit that Claims 1-3, 7-8, and 12-13 are not rendered unpatentable by *Pearce* and respectfully traverse Examiner's rejection in view of the arguments submitted herein.

Anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed

RPS920000109US1

Amendment D

09/847,085

- 6 -

invention as well as disclosing structure which is capable of performing the recited functional limitations. RCA Corp. v. Applied Digital Data Systems, Inc., 730 F.2d 1440, 221 USPQ 385 (Fed. Cir. 1984); W.L. Gore and Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983).

Pearce discloses a system and method of ensuring "that a disk drive that is inserted into a computer system while the operation system is active is the drive previously used to boot the operating system" (col. 2, lines 5-9). System management mode (SMM) software is "invoked which powers on the hard drive and reads unique drive information from the hard drive" (col. 2, lines 13-16). If the computer system determines that the disk drive currently inserted into the computer system is not the drive that was used to boot the operating system, the system and method disclosed in *Pearce* queries the user to determine if the disk drive has been changed and repeats the process until the disk drive that was used during boot time is re-inserted into the computer system (Figure 6).

Nothing in *Pearce* teaches or suggests "interrogating a boot device for device password" and "in response to the boot device supplying said device password corresponding to that of a trusted boot device, booting the data processing utilizing the boot device . . ." (Claim 1). According to paragraph 19 of the present Office Action, Examiner states that "[t]he hard drive of *Pearce* is used to boot the system, only upon the unique drive identification and serial number, this is how the system of *Pearce* determines whether the boot device is a trusted boot device".

Applicants respectfully disagree with Examiner's interpretation of *Pearce*. Merely obtaining the unique drive identification of serial number of the hard disk drive does not in itself determine whether the boot device is a trusted boot device. In fact, *any* hard disk drive can be utilized to boot the computer system disclosed in *Pearce*. The only determination that the system disclosed in *Pearce* makes is whether or not the hard disk drive present in the system after the system resumes is the same as the hard disk drive previously utilized to boot the system (col. 2, lines 28-50).

For example, consider that the system disclosed in *Pearce* may accept different hard disk drives that may be utilized to boot the system. If an individual wished to compromise the system, the individual can merely remove a first hard disk drive previously installed in the system and replace the first hard disk drive with a second hard disk drive. Then, when the individual turns on the system, the system will retrieve the unique drive identification and serial number from the second hard disk drive. The system will then boot, utilizing the information stored on the second hard disk drive, and allow the individual to gain access to the system.

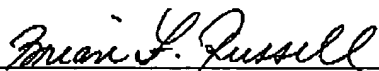
The system disclosed in *Pearce* makes no determination of whether the second hard disk drive (supplied by the hypothetical individual wishing to compromise the system) is a "trusted boot device", or a device that has been authorized to boot the system (Specification, page 8, lines 6-9). In fact, the individual would successfully gain access to the system by merely substituting the first hard disk drive with the second hard disk drive, as long as the substitution is performed pre-boot. The determination made in *Pearce* when comparing the unique drive identification and serial numbers merely is performed to determine if the hard disk drive used to boot the system is the same hard disk drive present on system resume (NOT boot) (*Pearce*, col. 2, lines 28-50). Thus, *Pearce* does not disclose a determination of whether the present hard disk drive is a "trusted boot device".

In light of the preceding argument, Applicants believe that independent Claim 1, similar Claims 7 and 12 and all dependent claims are not anticipated by *Pearce*. Furthermore, because *Pearce* discloses a system and method of ensuring "that a disk drive that is inserted into a computer system while the operation system is active is the drive used to boot the operating system" (col. 2, lines 5-9), there is no teaching or suggestion that would prompt a person with ordinary skill in the art to modify *Pearce* to perform the features of "interrogating a boot device for password information" and "in response to the boot device supplying password information corresponding to that of a

trusted boot device, booting the data processing utilizing the boot device . . ." as recited in Claim 1 and similar Claims 7 and 12.

Applicants believe that the above arguments overcome the pending rejections and respectfully request a notice of allowance for the present application. Applicants further respectfully request the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,



Brian F. Russell
Reg. No. 40,796
Dillon & Yudell LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)